What is Claimed is:

1. A method for verifying the source of an article of manufacture, said method comprising the steps of:

a) preparing a label, said label including information relating to said article;

b) encrypting at least a portion of said information included on said label;

c) securely associating said article, said label, and a tangible representation of said encrypted information.

2. A method described in Claim 1 wherein said information included on said label includes verifying information for protecting against unauthorized use of duplicate labels.

3. A method as described in Claim 2 wherein said verifying information includes information consisting of: an expiration date, a unique identification of said article of manufacture, an identification of a provider of said article of manufacture, or information describing said article of manufacture.

4. A method as described in Claim 1 wherein said label further includes an unreproduceable pattern and said method includes the further step of including a description of said unreproduceable pattern with said information included on said label.

5. A method as described in Claim 4 wherein said unreproduceable pattern is formed from magnetic fibers embedded in said label.

6. A method as described in Claim 4 wherein said encrypted information is encrypted with a first private key of a first public/private key pair and a corresponding first public key is available to parties who wish to validate the source of said article.

7. A method as described in Claim 6 wherein a trusted third party provides a party producing said label with said first private key and with an encryption of said first public key by a second private key kept secret by said trusted third party, said producing party including said encryption of said first public key with said label and said trusted third party providing a corresponding second public key to parties who wish to verify the source of said article; whereby said parties can recover said first public key from said label so that articles from a large number of different sources can be verified without the need to maintain a corresponding database of public keys.

8. A method as described in Claim 1 wherein said encrypted information is encrypted with a first private key of a first public/private key pair and a corresponding first public key is available to parties who wish to validate the source of said article.

9. A method as described in Claim 8 wherein a trusted third party provides a party producing said label with said first private key and with an encryption of said first public key by a second private key kept secret by said trusted third party, said producing party including said encryption of said first public key with said label and said trusted third party providing a corresponding second public key to parties who wish to verify the source of said article; whereby said parties can recover said first public key from said label so that articles from a large number of different sources can be verified without the need to maintain a corresponding database of public keys.

10. A method for labeling an article, said method comprising the steps of:

a) providing a label for said article, said label having an unreproduceable pattern;

b) scanning said label to generate a signal representative of said unreproduceable pattern;

c) encrypting at least a portion of said signal;

d) securely associating a tangible representation of said encrypted portion of said signal, said article and said label.

11. A method for verifying a label, said label having an unreproduceable pattern, and a tangible representation of at least an encrypted portion of a signal description of said unreproduceable pattern being securely associated with said label, said method comprising the steps of:

a) scanning said label to generate a second signal descriptive of said unreproduceable pattern;

b) reading said tangible representation to recover said encrypted portion of said descriptive signal;

c) decrypting said encrypted portion, or encrypting a corresponding portion of said second signal; and

d) comparing said decrypted portion of said descriptive signal with said corresponding portion of said second signal, or comparing said encrypted portion of said descriptive signal with said corresponding encrypted portion of said second signal, to verify said label.